CLAIMS

1. A method of validating software code provided to a user entity by a software provider, wherein:

- the user entity encrypts first data, provides it to the software provider, and receives back a valid indication that the code is valid only if the software provider has been able to correctly decrypt the encrypted first data, such decryption only being possible using an appropriate decryption key provided by a party with rights in the software code;
- the user entity encrypts the first data using, as encryption parameters, both an encryption key string comprising said software code or a representation thereof, and public data of said party;
- the said appropriate decryption key is provided by said party to the software provider only if the software code provided to the user entity is valid, generation of this key by the party using both private data related to said public data, and the encryption key string or a corresponding reference string based on a reference version of the software code.

2. A method according to claim 1, wherein the first data is a nonce.

3. A method according to claim 1, wherein said valid indication that the code is valid is said first data correctly decrypted from the encrypted first data.

4. A method according to claim 1, wherein said party receives the encryption key via the software provider and uses it to carry out at least one validation check of the software code provided to the user entity; the party also using the received encryption key string, together with said private data, to generate the said appropriate decryption key with the proviso that the decryption key is only generated or only provided to the software provider, if the or each validation check is satisfactory.

5. A method according to claim 4, wherein said at least one validation check comprises at least one of:

- a check on the integrity of the software code;
- a check on the right of the software provider to provide the software code to the user entity.

6. A method according to claim 4, wherein the encryption key string further comprises second data.

7. A method according to claim 6, wherein the second data is a random number.

8. A method according to claim 1, wherein said party is arranged to derive a decryption key using said reference string and said private data, whereby this key only serves as said appropriate decryption key if the software code provided to the user entity is the same as said reference version.

9. A method according to claim 8, wherein the encryption key string further comprises second data, the second data being provided to said party which uses it, together with the reference version of the software code or a representation thereof, to generate the decryption key.

10. A method according to claim 9, wherein the second data is a random number.

11. A computer system comprising first, second and third computing entities, wherein:

- the first computing entity is arranged to receive software code from the second computing entity and to encrypt a first data set using, as encryption parameters, both an encryption key string comprising a second data set corresponding to the software code provided by the second computing entity or a representation of that code, and public data of a party having rights in the software code; the first computing entity being further arranged to provide the encrypted first data set to the second computing entity whereby to receive back a valid indication that the code is valid only if the second computing entity is able to correctly decrypt the encrypted first data, such decryption only being possible using an appropriate decryption key provided by the third computing entity;

- the third computing entity is associated with said party having rights in the software code and is arranged to provide the said appropriate decryption key to the second computing entity only if the software code provided to the first computing entity is valid, the third computing entity being arranged to generate this key using both private data related to said public data, and the encryption key string or a corresponding reference string based on a reference version of the software code.

12. A computer system according to claim 11, wherein the first data set is a nonce.

13. A computer system according to claim 11, wherein the second computing entity is arranged to operate a web site and to provide said software code via the web site.

14. A computer system according to claim 11, wherein said party is the software producer.

15. A computer system according to claim 11, wherein the encryption key string further comprises a third data set.

16. A computer system according to claim 15, wherein the third data set is a random number.

17. A computer system according to claim 15, wherein the third computing entity is arranged to derive a decryption key using said reference string and said private data whereby this key only serves as said appropriate decryption key if the software code provided to the first computing entity is the same as said reference version, the third computing entity being arranged to receive the third data set from the second

computing entity and to form said reference string using the received third data set and the reference version of the software code or a representation thereof.

18. A computer system according to claim 11, wherein the third computing entity is arranged to receive said encryption key string via the second computing entity and to use it to carry out validation of the software code provided to the first computing entity, the third computing entity being arranged to derive the decryption key using said encryption key string and/or to provide the decryption key to the second computing entity, only after satisfactory validation of the software code whereby the decryption key, if provided to the second computing entity, is said appropriate decryption key.

19. A computer system according to claim 18, wherein the third computing entity is arranged to carry out validation of the software code by checking at least one of:

- the integrity of the software code;
- the right of the second computing entity to provide the software code to the first computing entity.

20. A computer system comprising a first computer entity for deriving an encryption key string using a first data set corresponding to software code or a representation of software code provided by a second computer entity and encrypting a second data set with the encryption key string; communication means for providing the encrypted second data set to the second computer entity; wherein a third computer entity associated with a third party having rights in the software code is arranged to provide to the second computer entity a decryption key derived using the first data set to allow decryption of the encrypted second data set.

21. A computer system according to claim 20, wherein the communication means provides the encryption key string to the third computer entity to allow validation of the first data set.

22. A computer system according to claim 21, wherein the third computer entity provides the decryption key to the second computer entity on validation of the first data set.

23. Apparatus comprising:

- first means for downloading software code over a network from a software provider,
- second means for encrypting first data using both public data of a party with rights in the software, and an encryption key string comprising said software code or a representation thereof;
- third means for providing the encrypted first data and said encryption key string to the software provider;
- fourth means for receiving back third data from the software provider, and
- fifth means for comparing the third data with the first data, and for generating an indication that the software code is valid if the first and third data match.

24. Apparatus according to claim 23, wherein the first data is a nonce.

25. Apparatus according to claim 23, wherein the encryption key string further comprises at least one of a random number and a time indication.

26. A computer program product arranged to condition computing apparatus, when installed thereon, to provide:

- means for encrypting first data using both an encryption key string comprising software code downloaded by the apparatus from a software provider or a representation of that code, and public data of a party with rights in the software code;
- means for providing the encrypted first data and said encryption key string to the software provider;
- means for receiving back third data from the software provider, and

- means for comparing the third data with the first data, and for generating an indication that the software code is valid if the first and third data match.